Amendments to the Claims:

This listing of the claims will replace all prior versions and listings of the claims in the application:

Listing of Claims:

1. (Currently Amended) A method for controlling the disclosure time of information by a publisher [[(10)]] to one or more recipients [[(31)]] comprising:

a trusted body [[(30)]] generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key [[(32)]] and a decryption key [[(34)]];

the trusted body [[(30)]] providing a digital certificate [[(20)]] signed with a private key [[(26)]] of the trusted body [[(30)]] providing the publisher [[(10)]] with the encryption key [[(32)]] prior to the specified date and time;

the publisher [[(10)]] using the encryption key [[(32)]] to encrypt data [[(15)]];

the recipient [[(31)]] obtaining the encrypted data [[(15)]]; and

the trusted body [[(30)]] making the decryption key [[(34)]] available to the recipient [[(31)]] at the specified date and time.

2. (Currently Amended) A method as claimed in claim 1, wherein the publisher [[(31)]] verifies the signature [[(25)]] on the digital certificate [[(20)]] with the public key of the trusted body [[(30)]].

3. (Currently Amended) A method as claimed in claim 1 ~~or claim 2~~, wherein the encryption key [[(32)]] is a public key and the decryption key [[(34)]] is a private key in a public key infrastructure.

4. (Currently Amended) A method as claimed in ~~any one of claims 1 to 3~~ claim 1, wherein the trusted body [[(30)]] creates an asymmetrical key pair for a specified date and time on demand from a publisher [[(10)]].

5. (Currently Amended) A method as claimed in claim 1~~any one of the preceding claims~~, wherein the trusted body [[(30)]] generates one key pair for a specified date and time.

6. (Currently Amended) A method as claimed in claim 1~~any one of claims 1 to 4~~, wherein the trusted body [[(30)]] generates one or more key pairs for a specified date and time, generating a new key pair for each of a plurality of publishers [[(10)]].

7. (Currently Amended) A method as claimed in claim 6, wherein each of the one or more publishers [[(10)]] has a password [[(50)]] issued by the trusted body [[(30)]] for preventing disclosure of the decryption key [[(34)]].

8. (Currently Amended) A method as claimed in claim 1~~any one of the preceding claims~~, wherein the decryption key [[(34)]] is encrypted with a public key [[(55)]] and only recipients [[(31)]] with the corresponding private key [[(53)]] can obtain the decryption key [[(34)]].

9. (Currently Amended) A system for controlling the disclosure time of information comprising:

a publisher [[(10)]];

a trusted body [[(30)]];

an asymmetrical key pair for a specified date and time of disclosure with an encryption key [[(32)]] and a decryption key [[(34)]];

a digital certificate [[(20)]] signed with a private key [[(26)]] of the trusted body [[(30)]] providing the publisher [[(10)]] with the encryption key [[(32)]] prior to the specified date and time; and

means for making the decryption key [[(34)]] available at the specified date and time.

10. (Currently Amended) A system as claimed in claim 9, including one or more recipients [[(31)]] with means for obtaining data [[(15)]] encrypted with the encryption key [[(32)]] from the publisher [[(10)]] prior to the specified date and time and means for obtaining the decryption key [[(34)]] at or after the specified date and time.

11. (Currently Amended) A system as claimed in claim 9 ~~or claim 10~~, wherein the certificate [[(20)]] includes the specified date and time, the encryption key value [[(32)]], and the name of the trusted body [[(30)]].

12. (Currently Amended)A system as claimed in claim 9~~any one of claims 9 to 11~~, wherein the encryption key [[(32)]] is a public key and the decryption key [[(34)]] is a private key in a public key infrastructure.

13. (Currently Amended) A system as claimed in claim 9~~any one of claims 9 to 12~~, wherein there is a single key pair for a specified date and time.

14. (Currently Amended) A system as claimed in claim 9~~any one of claims 9 to 12~~, wherein there is a plurality of publishers [[(10)]] and one or more key pairs for a specified date and time, a different key pair for each of the plurality of publishers [[(10)]] for the specified date and time.

15. (Currently Amended) A system as claimed in claim 14, wherein each of the plurality of publishers [[(10)]] has a password [[(50)]] issued by the trusted body [[(30)]] for preventing disclosure of the decryption key [[(34)]].

16. (Currently Amended) A system as claimed in claim 9~~any one claims 9 to 15~~, wherein the decryption key [[(34)]] is encrypted with a public key [[(55)]] and only recipients [[(31)]]

with the corresponding private key [[(53)]] can obtain the decryption key [[(34)]].

17. (Currently Amended) A system as claimed in claim 9~~any one of claims 9 to 16~~, wherein the trusted body [[(30)]] has one or more agents who act on behalf of the trusted body [[(30)]].

18. (Currently Amended) A system as claimed in claim 17, wherein an agent for the trusted body [[(30)]] is a smart card having an internal clock for providing the decryption key [[(34)]] to a recipient [[(31)]].

19. (Currently Amended) A system as claimed in claim 10~~any one of claims 10 to 18~~, wherein the trusted body [[(30)]] is accessible by the publisher [[(10)]] and the recipients [[(31)]] via a communication network.

20. (Currently Amended) A method for controlling the disclosure time of information by a publisher [[(10)]] to one or more recipients [[(31)]] comprising:

a trusted body [[(30)]] generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key [[(32)]] and a decryption key [[(34)]];

the trusted body [[(30)]] providing the publisher [[(10)]] with the encryption key [[(32)]] prior to the specified date and time;

the publisher [[(10)]] using the encryption key [[(32)]] to encrypt data [[(15)]];

the recipient [[(31)]] obtaining the encrypted data [[(15)]]; and

the trusted body [[(30)]] making the decryption key [[(34)]] available to the recipient [[(31)]] at the specified date and time;

wherein the trusted body [[(30)]] generates one or more key pairs for a specified date and time, generating a new key pair for each of a plurality of publishers [[(10)]].

21. (Currently Amended) A method as claimed in claim 20, wherein each of a plurality of publishers [[(10)]] has a password [[(50)]] issued by the trusted body [[(30)]] for preventing disclosure of the decryption key [[(34)]] for a specified date and time for that publisher [[(10)]].

22. (Currently Amended) A method as claimed in claim 20~~ or claim 21~~, wherein the decryption key [[(34)]] is encrypted with a public ke y [[(55)]] and only recipients [[(31)]] with the corresponding private key [[(53)]] can obtain the decryption key [[(34)]].

23. (Currently Amended) A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the steps of ~~any one of~~ claim 1 ~~20 to claim 8 22~~ when said product is run on a computer.

24. (Currently Amended) An information distributing service for controlling the disclosure time of information by a publisher [[(10)]] to one or more recipients [[(31)]] comprising:

a trusted body [[(30)]] generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key [[(32)]] and a decryption key [[(34)]];

the trusted body [[(30)]] providing a digital certificate [[(20)]] signed with a private key [[(26)]] of the trusted body [[(30)]] providing the publisher [[(10)]] with the encryption key [[(32)]] prior to the specified date and time;

the publisher [[(10)]] using the encryption key [[(32)]] to encrypt data [[(15)]]; the recipient [[(31)]] obtaining the encrypted data [[(15)]]; and

the trusted body [[(30)]] making the decryption key [[(34)]] available to the recipient [[(31)]] at the specified date and time.